



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,400	11/03/2003	Anne Elizabeth Dudfield	12221-018001	6347
26161	7590	09/10/2007		
FISH & RICHARDSON PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			EXAMINER PARTHASARATHY, PRAMILA	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 09/10/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

12

# Office Action Summary

Application No.

10/701,400

Applicant(s)

DUDFIELD ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 23 June 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This action is in response to the communication 06/23/2004. No preliminary amendments to the claims were filed. Claims 1 – 33 are currently pending.

#### ***Double Patenting***

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 24 of copending application 10/701,154. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 33 correspond to the claims of 1 – 24 of the copending application, except in the instant claims the elements “determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously” referred in the copending claims as “to collect connection information to identify host connection pairs from packets that are sent between nodes

on a network". Copending claims recite, "determine at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusion" which encompasses the instant application claims "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the host are in roles that are not normal for the hosts" and "anomalies includes determining if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table". Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC)* 29 USPQ2d 2010 (12/3/1993).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

3. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 22 of copending application 10/701,353. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 33 correspond to the claims of 1 – 22 of the copending application, except in the instant claims the elements "determining whether that one host attempting to gain access has

accessed the other host accessed previously; and if that one host has not accessed the other host previously” referred in the copending claims as “detecting scans emanating from hosts; analyzing records of scans to determine receivers of a scan and to determine which of those receivers of scans later became sources for a subsequent scan”. Copending claims recite, “analyzing scan anomalies for the sets of the hosts scanned” and “executing a scan detection process to determine hosts that were targets of scans” which encompasses the instant application claims “determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the host are in roles that are not normal for the hosts”. Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC)* 29 USPQ2d 2010 (12/3/1993).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

4. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 36 of copending application 10/701,356. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 –

33 correspond to the claims of 1 – 36 of the copending application, except in the instant claims the elements “retrieving connection pairs from a connection table for a host that is attempting to gain access to another host” referred in the copending claims as “a memory storing a connection table that maps each node of network to a host object, the connection table stores information about traffic to or from the node”. Copending claims recite, “a process to aggregate anomalies into the network events according to connection patterns” which encompasses the instant application claims “determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event”. Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC)* 29 USPQ2d 2010 (12/3/1993).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

5. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 21 of copending application 10/701,376. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 –

33 correspond to the claims of 1 – 21 of the copending application, except in the instant claims the elements “determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously” referred in the copending claims as “determining whether a variance in the parameter for the found anomaly exceeds a threshold; and if the variance exceeds that threshold collecting those found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network”. Copending claims recite, “detecting conditions in a network ... further comprising determining event severity” which encompasses the instant application claims “determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access”. Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC) 29 USPQ2d 2010 (12/3/1993)*).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

6. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 36 of copending application 10/701,404. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 33 correspond to the claims of 1 – 36 of the copending application, except in the instant claims the elements “retrieving connection pairs from a connection table for a host that is attempting to gain access to another host” referred in the copending claims as “adding host-pair connection records to a connection table each time a host accesses another host” and “wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table”. Copending claims recite, “determining from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event” which encompasses the instant application claims “determining whether the connection requests use the transport control protocol (TCP)” and “determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access”. Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such



are unpatentable for obvious-type double patenting (*In re Goodman (CAFC)* 29 USPQ2d 2010 (12/3/1993).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1 – 33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim(s) 31 – 33 are not limited to tangible embodiments as they recite configured for “determining”, “receiving” and “sending” functions, which do not define any structural and functional interrelationships between the method, program or instructions and other claimed aspects of the invention, which permits the program’s functionality to be realized.

The rejection of the base claim is necessarily incorporated into the dependent claims.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**8.** Claims 1- 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (US Patent 7,234,168).

**9.** As per Claims 1, 12 and 23, Gupta teaches “retrieving connection pairs from a connection table for a host that is attempting to gain access to another host; determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously, determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access” (Column 6 lines 3 – 42 and Column 7 lines 10 – 60).

**10.** As per Claims 2, 13 and 24, Gupta teaches “wherein determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts” (Column 7 lines 29 – 45).

**11.** As per Claims 3, 14 and 25, Gupta teaches “determining other anomalies includes determining whether the connection request uses the transport control protocol (TCP) (Column 7 lines 50 – 60)”.

**12.** As per Claims 4, 15 and 26, Gupta teaches “determining other anomalies includes determining whether the connection requests use ports that are not well-known thus indicating a possible Trojan virus attack” (Column 9 lines 50 – 59).

**13.** As per Claims 5, 16 and 27, Gupta teaches “determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event” (Column 23 lines 21 – 29).

**14.** As per Claims 6, 17 and 28, Gupta teaches “wherein determining other anomalies includes determining whether the connection requests use ports that have not been used previously” (Column 6 lines 3 – 11).

**15.** As per Claims 7, 18 and 29, Gupta teaches “wherein determining other anomalies includes determining if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table” (Column 7 lines 19 – 28).

**16.** As per Claims 8, 19 and 30, Gupta teaches “determining whether conditions exist to decrease the severity assigned to an event” (Column 21 lines 21 – 39).

17. As per Claims 9, 20 and 31, Gupta teaches “determining whether conditions exist to decrease the severity assigned to an event, comprises: determining whether the hosts are in roles that commonly access each other's hosts” (Column 21 lines 21 – 39).

18. As per Claims 10, 21 and 32, Gupta teaches “determining whether conditions exist to decrease the severity assigned to an event, comprises: determining whether the host being connected to commonly receives connections from new hosts” (Column 21 lines 21 – 39).

10. As per Claims 11, 22 and 33, Gupta teaches “determining if other anomalies in the connection patterns of each host exist further comprises: determining whether conditions exist to decrease the severity assigned to an event; and if an event is still indicated, sending an event warning message with a determined level of severity to an operator” (Column 21 lines 21 – 39).

### ***Conclusion***

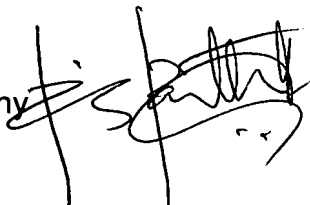
The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy  
August 26, 2007.

A handwritten signature in black ink, appearing to be 'P. Parthasarathy', written over a horizontal line.